

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Arizona's state court system has [suffered](#) a phishing-led cyberattack after an employee clicked a malicious link. Attackers copied backup files containing protective-order records and more than 150,000 Foster Care Review Board reports dating back to 2010, exposing personal and case-related information belonging to current and former participants.
- Japanese car-sharing service Times Car has [disclosed](#) a data breach affecting approximately 6.6 million current and former accounts. Exposed information includes personal data, while identity-verification documents, including driver's-license images, were exposed for about 1.6 million accounts. Payment card information was not affected.
- South Africa's air navigation provider has [suffered](#) a ransomware attack affecting operational technology supporting aviation weather services. Preliminary findings identified suspicious activity in weather-related environments, while separate reporting cited possible data theft. The provider has sought independent digital forensics to determine the scope of the incident.
- Fakturownia, a Polish online invoicing platform used by more than 600,000 businesses, has [disclosed](#) a data breach after an attacker exploited a system vulnerability. Copied information included account and company data, password hashes, bank account details, authentication tokens, contractor information, and portions of invoices stored on the platform.

AI THREATS

- Researchers [observed](#) autonomous AI agents attempting rudimentary hacking techniques while gathering public information from US and Canadian government websites. Activity included failed SQL injection attempts against the US Department of Education and Library and Archives Canada. Officials reported no compromise, while the origin of the agents remains unconfirmed.
- Researchers [demonstrated](#) that malicious Custom GPTs hosted on ChatGPT were used in a ClickFix campaign to deliver remote access malware. Victims were redirected to a Google Sites page and tricked into running commands. Huntress investigated at least 40 related incidents, including two confirmed infections that began through Custom GPTs.
- Researchers [outlined](#) how JadePuffer, an AI-enabled threat actor tracked as Storm-3168, used compromised Azure service principals to automate cloud reconnaissance and destructive actions. The activity included deleting storage and application resources, targeting backup-related assets, and attempting to retrieve access keys, reflecting agent-driven post-compromise operations in cloud environments.

VULNERABILITIES AND PATCHES

- Citrix has [issued](#) fixes for critical NetScaler vulnerabilities CVE-2026-88771-2, affecting NetScaler ADC and Gateway. Attackers have exploited the flaws to gain remote access, deploy web shells and tunneling malware, steal credentials, and move from exposed appliances into internal networks.

Check Point IPS provides protection against these threats (Citrix NetScaler Multiple Products Buffer Overflow (CVE-2026-88772), Citrix NetScaler Multiple Products Command Injection (CVE-2026-88771))

- Cisco has [alerted](#) about CVE-2026-76504, a critical (CVSS 9.8) vulnerability in Catalyst SD-WAN Manager. The flaw allows an unauthenticated remote attacker to send crafted requests and gain administrator access. Cisco reported active exploitation and stated that no fixes are available.

Check Point IPS provides protection against this threat (Cisco Catalyst SD-WAN Manager Authentication Bypass (CVE-2026-76504))

- Apple has [patched](#) CVE-2026-86950, a CoreGraphics memory corruption vulnerability affecting iPhones, iPads, and Macs. Processing a malicious image or PDF can allow arbitrary code execution. Apple reported exploitation in highly targeted attacks and addressed the flaw through improved bounds checking across affected iOS, iPadOS, and macOS releases.
- GitLab has [released](#) patches for CVE-2026-90970, a critical AI Gateway vulnerability rated CVSS 9.9. Authenticated Duo Agent Platform users can escape the prompt-template sandbox and execute arbitrary commands on the AI Gateway host.

THREAT INTELLIGENCE REPORTS

- Researchers [documented](#) Warlock ransomware attacks exploiting SharePoint ToolShell vulnerabilities against organizations in the utilities, telecom, government and education sectors. The group used compromised SharePoint servers for initial access, disabled endpoint protection on dozens of systems, and deployed ransomware across at least 33 hosts during one intrusion.
- Researchers [exposed](#) a China-nexus espionage campaign tracked as UAT-11587 targeting government and policy organizations across Asia. The group deployed the Antino backdoor through spear-phishing and tailored decoy documents. Antino uses Microsoft 365 services for command and control, file transfer, system reconnaissance, command execution, and persistence.
- Researchers have [uncovered](#) TA419, a China-aligned espionage actor targeting US AI policy experts at think tanks, universities, and law firms. The group impersonates prominent economists and AI policymakers, builds rapport through benign emails, then redirects targets to phishing pages designed to steal Microsoft 365 credentials and session cookies.
- Researchers [mapped](#) Russia-linked Star Blizzard phishing campaigns targeting more than 100 organizations, primarily in the United States and United Kingdom. The actor uses a new RedFlick delivery technique to install the CosmicPulse backdoor through scheduled tasks, supporting espionage activity against governments, NGOs, think tanks, and organizations connected to Ukraine.